Could Critical Infrastructure Suffer from a PIPEDREAM?

02.15.2023 | By Hon. Chris Carney

During the past couple of years, multiple warnings of imminent cyberattacks have seemingly gone unheeded by critical infrastructure owners and operators. Is embracing a fantasy that they won't be attacked potentially a pipedream? Both figuratively and literally, the answer is "yes."

A report filed February 14, 2023 indicates how close multiple water and Liquefied Natural Gas (LNG) facilities came to being victims of a catastrophic Russian-based malware dubbed "PIPEDREAM." This malware is particularly pernicious because it can infect a broad range of industrial control systems (ICS) rather than a single, specific system. Described as a "'state-level', wartime capability," the PIPEDREAM malware has the capability of taking industrial control systems offline, creating a potentially disastrous outcome. Moreover, while earlier malwares could infect control systems through vulnerabilities in the system's software that could be remedied with a "patch," PIPEDREAM cannot be fixed with a patch because it takes advantage of the inherent capabilities built into the ICS itself.

However, because PIPEDREAM is such a potent malware, it is not known if it was actually prevented from infecting the control systems of water and LNG facilities, or if it is lying dormant waiting for the most opportune time to attack. At the very least, it is expected that PIPEDREAM will remain a tenacious threat that critical infrastructure owners and operators must take measures to thwart. The time for whistling past the graveyard is over.

The Cybersecurity and Infrastructure Security Agency (CISA) offers a number of ways to protect ICS from malware attacks.